(c) if x and y are not both 0 in Z/NZ, then $A\begin{pmatrix}x\\y\end{pmatrix}\neq\begin{pmatrix}0\\0\end{pmatrix}$;

(d) A gives a 1–to–1 correspondence of $(Z/NZ)^2$ with itself.

18. Prove that Every finite field has a generator. If g is a generator of F_q^*, then g^j is also a generator if and only if $g.c.d.(j,\ q-1) = 1$. In particular, that are a total of $\varphi(q-1)$ different generators of F_q^*.

19. Explain the ElGamal Cryptosystem.

20. Find factor 200819.

APRIL/MAY 2023

DEMA44A — NUMBER THEORY AND CRYPTOGRAPHY

Time : Three hours

Maximum : 75 marks

Arts & Science College T.V.Malai

SECTION A — (10 × 2 = 20 marks)

Answer ALL the questions.

1. Write Euclidean algorithm.

2. Define Congruence.

3. What do you mean by Cryptography?

4. What is Enciphering matrices?

5. Define Residues.

6. What is reciprocity?

7. Define Public key.

8. Expand RSA.

9. What is Pseudo primes?

10. Write the rho method.

SECTION B — ($5 \times 5 = 25$ marks)

Answer ALL the questions.

11. (a) Convert 10^6 to the base 2,7 and 26.

Or

(b) Find *g.c.d* (1547, 560).

12. (a) Find the inverse of $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2(Z/26Z)$.

Or

(b) Write down the affine enciphering transformation.

13. (a) If f is a prime number, prove that there are $(p^f - p)/f$ distinctmonic Irreducible polynomials of degree f in $F_p[X]$.

Or

(b) If Fq is a field of $q = p^f$ elements, prove that every element satisfy the equation $X^q - X = 0$ and Fq is precisely the set of roots of that equation. Also prove converse part.

14. (a) Explain the Diffie — Hellman key exchange system.

Or

(b) Find the discrete log of 28 to the base 2 in F_{37}^* using the Silver – Pohlig – Hellman Algorithm. (2 is a generator of F_{37}^*).

15. (a) Let d = *g.c.d.* (*k*, *m*), prove that there are exactly d elements in the group $\{g, g^2, g^3, \ldots g^m = 1\}$ which satisfy $x^k = 1$.

Or

(b) Let p be an odd prime and write $p-1 = 2^s t'$ odd. Prove that the number of $x \in \left(\frac{Z}{pZ}\right)^*$ which satisfy $fyx^{2^r t} \equiv -1 \bmod p$ (where t is odd) is equal to 0 if $r \geq s'$ and is equal to 2^r *g.c.d.* (t, t') if $r < s'$.

SECTION C — ($3 \times 10 = 30$ marks)

Answer any THREE questions.

16. State and prove Fermat's Little Theorem.

17. let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(Z/NZ)$ and set $D = ad - bc$.

Prove that the following are equivalent:

(a) g.c.d. $(D, N) = 1$;

(b) A has an inverse matrix;